

CLAIMS

1. (Currently Amended) A method for time-stamping a digital document comprising:
  - a. receiving identifying data associated with a document  $\Delta$  at an outside agency;
  - b. creating at said outside agency a first receipt based on said identifying data;
  - c. creating at said outside agency a second receipt based on a time indication that indicates when the document was received at the outside agency;
  - d. inserting a linking value into said first and second receipts that links the identifying data in the first receipt with the time indication in the second receipt;
  - e. certifying said first and second receipts at said outside agency using a cryptographic signature scheme.
2. (Original) The time-stamping method of claim 1 wherein said identifying data comprises a digital representation of at least a portion of said document.
3. (Original) The time-stamping method of claim 2 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.
4. (Original) The time-stamping method of claim 3 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.
5. (Original) The time-stamping method of claim 1 wherein said first receipt includes at least a portion of said identifying data and a nonce.

6. (Original) The time-stamping method of claim 1 wherein said first receipt includes a digital sequence generated by applying a pre-determined function to said identifying data.
7. (Original) The time-stamping method of claim 1 wherein one of said first and second receipts includes a user identification number associated with a user.
8. (Original) The time-stamping method of claim 7 wherein one of said first and second receipts includes a sequential record number.
9. (Currently Amended) A method for time-stamping a digital document comprising:
  - a. transmitting identifying data associated with said document to an outside agency;
  - b. receiving from said outside agency a first receipt signed by said outside agency using a cryptographic signature scheme, said first receipt including a first digital sequence generated based on said identifying data;
  - c. receiving from said outside agency a second receipt signed by said outside agency using a cryptographic signature scheme, said second receipt containing a second digital sequence based on a time indication that indicates when the document was received at the outside agency; and
  - d. wherein said first and second receipts include a linking value that links the identifying data in the first receipt with said time indication in the second receipt.
10. (Original) The time-stamping method of claim 9 wherein said identifying data comprises a digital representation of at least a portion of said document.

11. (Original) The time-stamping method of claim 10 wherein said identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of said document.
12. (Original) The time-stamping method of claim 11 wherein said digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of said document.
13. (Original) The time-stamping method of claim 9 wherein said first receipt includes at least a portion of said identifying data and a nonce.
14. (Original) The time-stamping method of claim 9 wherein said first receipt includes a digital sequence generated by applying a pre-determined function to said identifying data.
15. (Original) The time-stamping method of claim 9 wherein one of said first and second receipts includes a user identification number associated with a user.
16. (Original) The time-stamping method of claim 15 wherein one of said first and second receipts includes a sequential record number.
17. (Original) The time-stamping method of claim 9 wherein a common cryptographic signature scheme is used to sign both said first and second receipts.
18. (Original) The time-stamping method of claim 9 wherein different cryptographic signature schemes are used to sign said first and second receipts.

19. (Original) The time-stamping method of claim 9 wherein said linking value is a nonce value.